Aula 02

ALGORITMO DA DIVISÃO E MÁXIMO DIVISOR COMUM

META

Apresentar o algoritmo da divisão e estabelecer o conceito de máximo divisor comum.

OBJETIVOS

Definir a relação de divisibilidade em $\mathbb{Z}$.

Aplicar as propriedades da relação de divisibilidade.

Efetuar divisões com resto pequeno em $\mathbb{Z}$.

Resolver problemas que envolvam o conceito de máximo divisor comum de inteiros.

Calcular o máximo divisor comum de dois inteiros usando o algoritmo de Euclides.

PRÉ-REQUISITOS

O curso de Fundamentos de Matemática e a primeira aula.

INTRODUÇÃO

Olá! Que bom encontramos novamente! Espero que você tenha gostado e entendido a nossa primeira aula. Nela estudamos a estrutura de domínio ordenado dos inteiros onde discutimos várias das suas propriedades.

Nesta aula, daremos continuidade ao estudo destes números onde o resultado central é o algoritmo da divisão. Estabelecemos também o conceito de máximo divisor comum de inteiros cuja existência é uma conseqüência imediata do algoritmo da divisão.

A RELAÇÃO DE DIVISIBILIDADE E O ALGORITMO DA DIVISÃO

Definição 1. Dados $a, b \in \mathbb{Z}$, dizemos que a divide b se existe um inteiro c tal que $b = a.c$. Dizemos também que a é um divisor de b e ainda, que b é um múltiplo de a.

Escrevemos: $a|b$.

Assim, $a|b \Leftrightarrow \exists\ c \in \mathbb{Z}$ tal que $b = a.c$

Indicamos a negação de que a divide b escrevendo $a \nmid b$.

Exemplo 1. $5|20$, pois existe $4 \in \mathbb{Z}$ tal que $20 = 5.4$.

Proposição 1. São verdadeiras:

i) $a|a\ \ \forall a \in \mathbb{Z}$.

ii) Se $a|b$ e $b|c$ então $a|c, \forall\ a, b, c \in \mathbb{Z}$.

iii) Se $a|b$ e $c|d$ então $ac|bd, \forall\ a, b, cd \in \mathbb{Z}$.

iv) Se $a|b_1, b_2, \dots, b_n$ então $a|(b_1c_1 + b_2(2 + \cdots + b_nc_n), \dots, c_n \in \mathbb{Z}$.

v) Se $a, b \in \mathbb{Z}, a|b\ e\ b|c$ então $b = \pm a$.

vi) Se $a, b \in \mathbb{Z}, b \neq 0$ e $a|b$ então $|a| \leq |b|$.

Demonstração: Os itens i,ii e iii fazer como atividade.

iv) Existem $b_1, b_2, \dots, b_n \in \mathbb{Z}$ tal que $b_1 = ab_1^{'}, b_2 = ab_2^{'}, \dots, b_n = ab_n^{'}$, logo, $b_1c_1 + b_2c_2 + \cdots + b_nc_n = ab_1^{'}c_1 + ab_2^{'}c_2 + \cdots + ab_n^{'}c_n = a(b_1^{'}c_1 + b_2^{'}c_2 + \cdots + b_n^{'}c_n)$. Como $q = b_1^{'}c_1 + b_2^{'}c_2 + \cdots + b_n^{'}c_n$ é um inteiro segue que $a|(b_1c_1 + b_2c_2 + \cdots + b_nc_n)$.

v) $a|b \Longrightarrow \exists\ c_1 \in \mathbb{Z}$ tal que $b = ac_1. b|a \Rightarrow \exists\ c_2 \in \mathbb{Z}$ tal que $a = bc_2$. Assim, $a = (ac_1)c_2 \Rightarrow a = a(c_1c_2) \Rightarrow c_1c_2 = 1$. Temos então $c_1 = c_2 = 1$ ou $c_1 = c_2 = -1$. No primeiro caso, $b = a$ e no segundo, $b = -a$.

vi) Como $a|b \Rightarrow \pm a| \pm b$ temos que $|a|\big||b|$ e existe c positivo, $(isto\ é, 1 \leq c)$ tal que $|b| = |a|.c$, logo $|a| \leq |a|.c = b$.

Proposição 2. (Algoritmo da divisão). Sejam $a, d \in \mathbb{Z}$ sendo $d \neq 0$. Existem únicos $q, r \in \mathbb{Z}$ tais que $a = dq + r$ e $0 \leq r < |d|$.

Demonstração: Vamos supor inicialmente que $d > 0$. Para isto, consideremos o conjunto de números inteiros $A = \{u = a - dv | v \in \mathbb{Z}\} \cap \mathbb{Z}_{+}$. Então, A é não vazio $(a + d|a| \in A)$ e do princípio da boa ordem existem $r = m\acute{i}nA$ e $q \in \mathbb{Z}$ tais que $r = a - dq$. Ou melhor, existem $q, r \in \mathbb{Z}$ tais que $a = dq + r$ e $r \geq 0$. Além disto, $r < d$, pois se assim não fosse, teríamos $0 \leq r - d = a - d(q+1) \in A$ e $r - d < r = m\acute{i}nA$, contrariando a minimalidade de r. Quanto às unicidades de q e r; suponhamos que existam $q, r, q', r' \in \mathbb{Z}$ tais que $a = dq + r = dq'r'$ e $0 \leq r, r' < d$. Então $d(q - q') = r' - r$ e $d | r' - r$.

Se $r \leq r'$, temos $r + (r' - r) + (d - r' = d$ donde segue que $0 = r' - r < d$. Analogamente, se $r' \leq r$, $0 \leq r - r' < d$ e como $d | r - r'$ segue que $r - r' = 0$. Portanto $r = r'$ e conseqüentemente, $q = q'$.

Finalmente, se $d < 0$, temos $-d = |d| > 0$ e da primeira parte existem únicos $q', r' \in \mathbb{Z}$ tal que $a = -dq' + r'$ e $0 \leq r' < |d|$. Tomando $q = -q'$ e $r = r'$, temos a demonstração, concluída.

Exemplo 2. Para $a = -18$ e $d = -5$, o único par de inteiros que verifica o algoritmo da divisão é $q = 4$ e $r = 2$.

Os inteiros a, d, q, r, referidos no algoritmo da divisão são chamados, respectivamente, dividendo, divisor, quociente e resto. A operação que associa a cada par (a, d) o par (q, r) é chamada divisão e, quando $r = 0$ dizemos que a divisão é exata.

O MÁXIMO DIVISOR COMUM

Apesar de nem sempre ser possível dividir um inteiro por outro, de modo exato, o algoritmo da divisão nos garante em $\mathbb{Z}$, uma divisão. Esta propriedade implica em resultados algébricos notáveis e, o primeiro deles é a existência do máximo divisor comum que discutiremos agora.

Definição 2. Seja I um subconjunto não-vazio de $\mathbb{Z}$. Dizemos que I é um ideal se cumpre às seguintes condições:

i) $a, b \in I \Longrightarrow a - b \in I$

ii) $a \in \mathbb{Z}, b \in I \Rightarrow ab \in I$.

Notamos que $a \in I \Rightarrow a - a = 0 \in I$.

Se $a, b \in I$, por ii, $-b = (-1).b \in I$ e, por i, $a - (-b) = a + b \in I$.

Os conjuntos $O = \{0\}$ e $\mathbb{Z}$ são evidentemente ideais.Estes ,são chamados os ideais triviais de $\mathbb{Z}$.

Exemplo 3. Seja $d \in \mathbb{Z}$ e seja $I = (d) = \{du | u \in \mathbb{Z}\}$ o conjunto de todos os múltiplos de $d\ em\ \mathbb{Z}$. Este conjunto é um ideal de $\mathbb{Z}$, chamado ideal principal gerado por d. Com efeito, é fácil ver que a diferença entre dois múltiplos de d é o produto de um inteiro por um múltiplo de d, são múltiplos de d.

Observação: É comum usar as notações $< d >\ e\ d\mathbb{Z}$ para indicar o ideal (d).

Exemplo 2.2.4: Sejam $d_1, d_2, \dots, d_n \in \mathbb{Z}$. O to $I = \{d_1u_1 + d_2u_2 + \dots + d_nu_n | u_1, u_2, \dots, u_n \in \mathbb{Z}\}$ é um ideal, chamado ideal gerado por $d_1, d_2, \dots, d_n$.

Sejam $a, b \in I$, então, existem $u_1, u_2, \dots, u_n, v_1, v_2, \dots, v_n \in \mathbb{Z}$ tais que $a = d_1u_1 + d_2u_2 + \dots + d_nu_n$, $b = d_1v_1 + d_2v_2 + \dots + d_nv_n$ logo, $a - b = d_1(u_1 - v_1) + d_2(u_2 - v_2) + \dots + d_n(u_n - v_n)$ e como cada $u_i - v_i$ para $i = 1,2, \dots, n$ é inteiro, segue que $a - b \in I$.

Se $a \in \mathbb{Z}$ e $b = d_1v_1 + d_2v_2 + \dots + d_nv_n \in I$ então $ab = d_1(av_1) + d_2(av_2) + \dots + d_n(av_n)$ e como cada av_i para $i = 1,2, \dots, u$ é inteiro segue que $ab \in I$.

A proposição a seguir estabelece que todo ideal de $\mathbb{Z}$ é, na verdade, o conjunto de múltiplos de algum inteiro.

Proposição 3. Todo ideal de $\mathbb{Z}$ é principal.

Demonstração: Seja $I \subset \mathbb{Z}$ um ideal não nulo. Evidentemente $I \cap \mathbb{N} \neq \phi$ e do principio da boa ordem existe $d = mín(I \cap \mathbb{N})$.

Afirmamos: $I = (d)$. Com efeito, $(d) \subset I$, pois $ad \in I, \forall\ a\ \in \mathbb{Z}$. Seja a um elemento arbitrário em I, do algoritmo da divisão existem $q, r \in \mathbb{Z}$ tais que $a = dq + r$ e $0 \leq r < d$.

Sendo $r = a - dq \geq 0$, $a, d \in I$ temos $0 \leq r \in I$. Como $0 \leq r < d = \min\ (\mathrm{I} \cap \mathbb{N})$ segue que $r = 0$ e, $a = dq \in (d)$.

Portanto, $I = (d)$, como queríamos demonstrar.

Definição 3. Dados $d_1, d_2, \dots, d_n \in \mathbb{Z}$, não todos nulos, o máximo divisor comum de $d_1, d_2, \dots, d_n$ é, por definição, o maior dos divisores comuns de $d_1, d_2, \dots, d_n$.

Denotamos: $mdc(d_1, d_2, \dots, d_n)$.

Proposição 4. Sejam $d_1, d_2, \dots, d_n \in \mathbb{Z}$ não todos nulos. Então o $mdc(d_1, d_2, \dots, d_n)$ é o gerador positivo do ideal $(d_1, d_2, \dots, d_n)$.

Demonstração: Seja $d \in \mathbb{N}$ tal que $(d) = (d_1, d_2, \dots, d_n)$. Como, para cada $i \in \{1,2, \dots, n\}$, $d_i = 0.d_1 + \dots + 1.d_i + \dots + 0.d_n$, segue que $d_i \in (d)$ e conseqüentemente d é um divisor comum de $d_1, d_2, \dots, d_n$.

Seja $d' \in \mathbb{N}$ um outro divisor comum de $d_1, d_2, \dots, d_n$. Como, $d \in (d_1, d_2, \dots, d_n)$ existem $u_1, u_2, \dots, u_n \in \mathbb{Z}$ tais que $d = d_1u_1 + d_2u_2 + \cdots + d_nu_n$ (esta relação é conhecida como forma linear do máximo divisor comum). Desta relação segue que $d' \mid d$ e $d' \leq d$. Logo, $d = mdc(d_1, d_2, \dots, d_n)$.

Observação: A proposição acima garante que dados quaisquer $d_1, d_2, \dots, d_n \in \mathbb{Z}$ não todos nulas existe sempre o $mdc(d_1, d_2, \dots, d_n)$ e, na sua demonstração vimos também que a equação diofantina (equação algébrica que tem como universo de soluções números inteiros) $a_1x_1 + a_2x_2 + \cdots + a_nx_n = d$, tem solução.

Definição 4. Se $d_1, d_2, \dots, d_n \in \mathbb{Z}$ não são todos nulos e $mdc(d_1, d_2, \dots, d_n) = 1$, dizemos que $d_1, d_2, \dots, d_n$ são relativamente primos, primos entre si ou ainda, coprimos.

Exemplo 5. Se $d_1, d_2, \dots, d_n$ são inteiros para os quais existem $q_1, q_2, \dots, q_n \in \mathbb{Z}$ tais que $d_1q_1 + \cdots + d_nq_n = 1$ então esses inteiros são relativamente primos. Com efeito, notemos primeiro que não podem $d_1, d_2, \dots, d_n$ serem todos nulos, portanto, existe $d \in \mathbb{Z}$ tal que $d = mdc(d_1, d_2, \dots, d_n)$. Mas, da definição $d \mid d_1, d_2, \dots, d_n$, logo, $d \mid d_1q_1 + d_2q_2 + \cdots + d_nq_n$, isto é,$d \mid 1$ donde concluímos que $d = 1$.

Exemplo 6. Se $a = bq + r$, desde que existam, $mdc(a, b) = mdc(b, r)$. Escrevendo $mdc(a, b) = d$ e $mdc(b, r) = d'$, vamos provar que $d \mid d'$ e que $d' \mid d$ e, como estamos tratando de números positivos concluiremos que $d = d'$! Como $d \mid a, b$ temos que $d \mid a - bq$ ou seja $d \mid r$. Logo, $d \mid d'$. Analogamente, $d' \mid b, r$. Isto implica que $d' \mid b, bq + r$ e isto implica, ainda, que $d' \mid d$. Como $d' \mid d \ e \ d \mid d'$ temos que $d' = d$.

Proposição 2.2.5. (Algoritmo de Euclides para o cálculo do mdc). Sejam $a, b \in \mathbb{Z}_+^*$ com $a > b$. Sejam $a = bq_1 + r_1, b = r_1q_1 + r_2, r_1 = r_2q_3 + r_3, \dots, r_{n-1} = r_nq_{n+1} + r_{n+1}$ sucessivas divisões tais que $r_{n+1} = 0 < r_n < r_{n-1} < \cdots < r_2 < r_1 < b$. Então $mdc(a, b) = r_n$.

Demonstração: Segue do exemplo anterior que $mdc(a, b) = mdc(b, r_1) = mdc(r_1, r_2) = \cdots = mdc(r_n, 0) = r_n$

RESUMO

Nesta aula, estabelecemos o algoritmo da divisão, definimos o máximo divisor de dois ou mais inteiros e demonstramos a existência do máximo divisor comum como conseqüência do algoritmo da divisão.

ATIVIDADES

1. Sejam $a, b \in \mathbb{Z}$ tais que $a + b$ é par. Provar que $a - b$ também é par.
2. Ache $a, b, c \in \mathbb{Z}$ tais que $a \mid bc$, $a \nmid b$ e $a \nmid c$.
3. Se $a, b \in \mathbb{Z}$ são tais que $10a + b$ é um múltiplo de 7, prove que $a^3 - b^3$ também o é.

4. Prove que para todo inteiro positivo n:
   a) $9 \mid (10^n - 1)$.
   b) $8 \mid (3^{2n} - 1)$.
5. Determine $q, r \in \mathbb{Z}$ tais que $-10 = 3q + r$ e $0 \leq r < 3$.
6. Dados $a, d \in \mathbb{Z}$, $d > 0$, prove que existem únicos $q, r \in \mathbb{Z}$ tais que $a = dq + r$ e $2d \leq r < 3d$.
7. Sejam $a, b, c \in \mathbb{Z}\backslash\{0\}$. Prove que $mdc(a, b, c) = mdc(mdc(a, b), c)$.
8. Sejam $a, b \in \mathbb{Z}$ e suponha que existem $c, d \in \mathbb{Z}$ tais que $ac + bd = 1$. Provar que $mdc(a, b) = 1$.
9. Se $a, b, c \in \mathbb{Z}\backslash\{0\}$ são tais que $mdc(a, b, c) = 1$ e $a^2 + b^2 = c^2$, prove que a e b têm paridades diferentes e que c é impar.
10. Sejam $a, b \in \mathbb{Z}\backslash\{0\}$. Defina $m = mmc(a, b)$ como sendo o menor múltiplo comum positivo de a e b. Se $d = mdc(a, b)$, prove que $dm = ac$.
11. Use o algoritmo de Euclides para calcular $mdc(60,18)$.

COMENTÁRIOS DAS ATIVIDADES

Caro aluno, se você fez a primeira e segunda atividade, então entendeu a relação de divisibilidade. Quanto à terceira atividade, conseguiu? Então, além de entender a relação de divisibilidade você foi capaz de escrever $a^3 - b^3$ como sendo o produto $(a - b)(a^2 + ab + b^2)$ e usando a hipótese de que $7 \mid 10a + b$, concluir que $7 \mid a^2 + ab + b^2$.

Se você fez a quarta atividade, então você ou usou o principio de indução em n ou usou mais uma vez uma fatoração de tipo $a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1})$.

Quanto as quinta e sexta atividades, você deve ter usado fortemente, o algoritmo da divisão.

Se você resolveu as sétima e oitava atividades então, usou a definição de máximo divisor comum e deve ter usado o fato de que se $a, b \in \mathbb{Z}_+,\ a|b\ \ e\ \ b|a$ então $a = b$.

Na nona atividade, você deve ter notado que quadrado preserva a paridade e que soma de inteiros de mesma paridade é par.

Na décima atividade se você conseguiu fazê-la, deve ter usado preliminarmente que $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ e depois que m divide todos os múltiplos comuns de a e b.

Finalmente, a décima primeira atividade é uma aplicação direta do algoritmo da divisão e você não deve ter tido nenhuma dificuldade nesta atividade.

Se você não conseguiu resolver alguma destas atividades, reveja os conteúdos discutidos na aula e lembre-se que os tutores estão disponíveis para ajudar a tirar suas dúvidas.

REFERÊNCIAS

GONÇALVES, Adilson. Introdução à álgebra. 5. ed. Rio de Janeiro: IMPA, 2007. 194 p. (Projeto Euclides) ISBN.

HUNGERFORD, Thomas W. Abstract algebra: an introduction. 2nd. ed. Austrália: Thomson Learning, ©1997.

GARCIA, Arnaldo; LEQUAIN, Yves. Elementos de algebra. 3. ed. Rio de Janeiro: IMPA, 2005. 326 p. (Série: Projeto Euclides).